## Biotelemetrica: A Sabbatical Application

**Professor Richard Doyle**

**Penn State University**

**mobius@psu.edu**

**Brief Description of the Project:** I will research and write a book  on biotelemetrics, the emerging technologies of human identification at a distance. As US delegate to the global organizations concerned with emerging technological standards, I will conduct research and fieldwork for my fourth scholarly book. A draft of the book will be completed by Fall 2008.

---

*Whether clearly stated or not, that is what comes through in the explorers' chronicles and the work of researchers alike: society is inconceivable without the State; the State is the destiny of every society.*" **Pierre Clastres,** *Society Against the State*

"Biotelemetrics" names a diverse set of practices, technologies and disciplines oriented toward the non-invasive determination of human identity at a distance. Facial recognition, iris scans, gait signatures, and residual DNA analysis all compete with dozens of other technologies to render the holy grail of contemporary security science: a reliable and stealthy apprehension of human identity. Long a fascination of the Cold War Security State and science fiction, biotelemetrics is now a fundamental strategy in the "War on Terror". Already, global standards organizations - the International Electrotechnical Commission, the International Standards Organization, and the International Telecommunications Union - have sought to establish protocols governing the safety of biotelemetric technologies in contact with the diverse set of human populations likely to be surveyed by them. Civil liberties groups around the world have begun to have their own visions of the near future - a control society of Total Information Awareness in which privacy is nonexistent and human freedom atrophies, shrivels and disappears.

In August 2004, I was contacted by the International Electrotechnical Commission, a global standards organization that establishes protocols for electrical and informational technologies. Founded by Lord Kelvin in 1906, the IEC seeks to create stable and replicable protocols for the safe deployment of technologies around the planet. After reading my second book, *Wetwares: Experiments in PostVital Living (* revised and completed during my 200-2001 sabbatical leave), as well as my first book about the molecular biology and living systems, *On Beyond Living: Rhetorical Transformations of the Life Sciences,* IEC Technical Committee 25/ Working Group 5 sought my expertise in helping them develop "wetware protocols" to regulate the safe deployment of biotelemetric technologies. For the past two years I have acted as US Delegate to Technical Committee 25 Working Group 5 for the IEC, in close

association with the International Telecommunications Union, the UN body responsible for global information technology standards development. During that time I have completed my third book, <u>Ecodelic! Rhetoric, Plants and the Evolution of the Noosphere</u>, to be published by the University of Washington Press in a series on the Life Sciences, "In Vivo."

In this proposal, I seek as full year of sabbatical to research and write my fourth scholarly book, <u>Biotelemetrica or The (Da Vinci) Protocols: Towards a Peer to Peer Control Society?</u> My colleagues and I at the IEC and ITU are using the classic Da Vinci diagram to argue for one meter sphere around the human body free from "telebiometric browsing", and the book will chronicle our attempt and the emergence of biotelemetric technologies and standards. The book will be ethnographic in methodology, first person in perspective, and theoretically framed by discussions of control culture from Gustav Fechner to William S. Burroughs. <u>The (Da Vinci) Protocols</u> will seek to answer questions fundamental to scholarship and freedom of inquiry: How ought we respond to shifting concepts and practices of security driven by emerging and "disruptive" technologies such as peer to peer networks devoid of centralized control? What role can standards organizations play in a context seemingly dominated by corporate capital (telecommunications, information technologies) and the desires of intelligence services and nation-states for Total Information Awareness? .

A "peer to peer network", a network of computers without any centralized server or authority, forms the basis of my own evolving proposal for a "security commons." As shown in the diagram to the right, no central authority serves as the pivot point
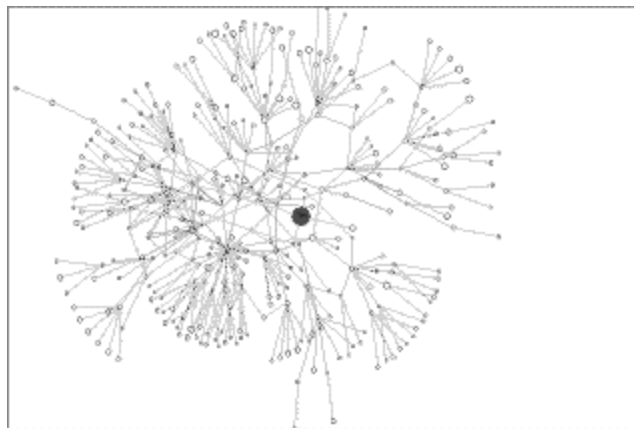


governing the network. It is instead a "distributed network architecture." My scheme for identity verification to be detailed and narrated in the book is a "modest proposal" ( Swift) that borrows this computer architecture and links computers as well as telebiometric devices into a network devoid of hierarchy or central governing authority – a security commons in response to the security state. I will pitch it in an Invited Lecture to Rice University's Computer and Information Technology Institute in early October, and I gave a brief talk about it here for my colleagues in Information Science and Technology.

In addition to a practical proposal for a security commons, <u>The DaVinci Protocols</u> will also provide insight and context for the emergence of new identity technologies. In the summer of 2005, I began interviewing scientists, psychologists and telecommunication engineers about the technical aspects of biotelemetrics and the sometimes surreal contexts in which these protocols and technologies are emerging. My role as a US Delegate to the IEC and a participant in the standards making process provides a unique location from which to survey, record, analyze and evaluate technological transformations already undermining traditional state based models of security and human identity. These standards driven paradigms suggest that highly distributed global organizations linked to protocols (such as the "http" protocol of Internet) offer more robust ecologies for security than the centralized models of sovereign power still relentlessly pursued by nation-states and large

telecommunication corporations. According to my preliminary research, my analysis is the first to articulate a scheme for the operation of "peer to peer" biotelemetric networks, and my research will seek to both flesh out and diagram any such system while thinking through the likely political and cultural effects of a radically decentralized ecology of security. Should I become convinced that this "p2p" model is even less conducive to the freedom of inquiry, travel and democratic deliberation than the currently repressive climate of the War on Terror, I will work to contest its implementation. I believe this peer to peer model to be "in the air" (catalyzed by the political and technological zeitgeist), so I am under no illusions that I will be the only analyst to stumble upon it.

This project will address readers interested in the cultural studies of science and technology, shifting markets in telecommunication, security, control culture, and the role of standards in shaping the political and economic landscape. As a rhetorician, the project will enable me to track the transformation of highly contested terms and documents into global standards, a technical Esperanto that often drives the globalization of technology markets and shifts understandings of global security. Duke University press has already expressed great interest in the project, and I will talk with Reynolds Smith, Duke's editor, at a conference in New York in November about the book proposal. Already, I have begun collaborations with faculty in Information Science and Technology at Penn State - with me they now host an open source IEC/ITU/ISO database devoted to mapping the thresholds of human sensory response for use in biotelemetric safety. A further description of the biometrica project, the database and the protocols can be found at  http://biotelemetrica.pbwiki.com/